UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

RUTH ALBRIGHT, individually and on behalf of those similarly situated, Plaintiff, v. **GEISINGER HEALTH and NUANCE COMMUNICATIONS, INC.**, Defendants.	Case No. 4:24-CV-1174-MWB **CLASS REPRESENTATION JURY** **TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Ruth Albright ("Plaintiff ") brings this Class Action Complaint ("Complaint"), on behalf of herself and all others similarly situated, against Defendants Geisinger Health ("Geisinger") and Nuance Communications, Inc. ("Nuance") (each a "Defendant" or collectively "Defendants") for failure to properly secure and safeguard Plaintiff's and Class Members' protected health information ("PHI") and personally identifiable information ("PII ") stored within Defendants' information network and alleging as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which is based on personal knowledge:

NATURE OF THE CASE

1. Entities that provide services in the healthcare industry and handle patients' sensitive, PHI and PII owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of patients' PHI and PII to unauthorized persons—especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a breach of private data manifests in a number of ways, including identity theft and financial fraud. The exposure of a person's PHI/PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and to take a number of additional prophylactic measures.

3. As a healthcare service provider, specifically a US-based business that provides electronic health records and practice management solutions to several healthcare organizations, Geisinger knowingly obtains sensitive patient PHI/PII and has a resulting duty to securely maintain such information in confidence.

4. As discussed in more detail below, Defendants breached their duty to protect the sensitive PHI/PII entrusted to them, and failed to abide by their own Privacy Policies (as discussed *infra*). As such, Plaintiff brings this Class action on behalf of herself and the approximately 1,000,000 other patients whose PHI/PII was accessed and exposed to unauthorized third parties during a data breach of Defendants' systems. (the "Data Breach"). The Data Breach was discovered by Geisinger which found that a former Nuance employee had accessed and acquired the PHI/PII of Plaintiff and Class members.

5. Indeed, Geisinger did not inform Plaintiff of the Data Breach until June 24, 2024, even though it became aware of the data breach on or about November 29, 2023.

6. Based on the public statements of Defendants to date, a wide variety of PHI/PII was implicated in the breach, including but not limited to, names, physical addresses, phone numbers, dates of birth, health insurance account information, Social Security numbers, provider taxpayer

identification numbers, and clinical information (e.g., medical history, diagnoses, treatment, dates of service, and provider names).

7. As a direct and proximate result of Defendants' inadequate data security, and their breach of their duty to handle PHI/PII with reasonable care, Plaintiff's PHI/PII has been accessed by hackers, posted on the dark web, and exposed to an untold number of unauthorized individuals.

8. Plaintiff is now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of her health privacy, and similar forms of criminal mischief, and such risk may last for the rest of her life. Consequently, Plaintiff must devote substantially more time, money, and energy to protect herself, to the extent possible, from these crimes.

9. Plaintiff, on behalf of herself and others similarly situated, brings claims for negligence, negligence *per se*, breach of fiduciary duty, breach of confidences, breach of an implied contract, unjust enrichment, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

10. To recover from Defendants for her sustained, ongoing, and future harms, Plaintiff seeks damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendants to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PHI/PII accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PHI/PII possessed by Defendants; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

Plaintiff

11. Plaintiff Ruth Albright is an adult individual and, at all relevant times herein, a

resident and citizen of Pennsylvania, residing in Millheim, Pennsylvania. Plaintiff is a victim of the Data Breach.

12. Plaintiff is a patient of Geisinger and her information was stored with and handled by Defendants as a result of her dealings with Defendants.

13. On or about June 24, 2024, Plaintiff was notified of the Data Breach and of the impact to her PHI/PII via letter from Defendants.

14. As a result of Defendants' conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

Defendants

15. Defendant Geisinger Health is a Pennsylvania nonprofit corporation with its principal place of business at 100 North Academy Avenue, Danville, Pennsylvania 17822.

16. Defendant Nuance Communications, Inc. is a Delaware corporation with its headquarters located at 1 Wayside Road, Burlington, Massachusetts 01803. It may be served through its registered agent: Corporation Service Company, 84 State Street, Boston Massachusetts 02109.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

18. Plaintiff will seek leave of court to amend this Complaint to reflect the true names

and capacities of the responsible parties when their identities become known.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendants' states of citizenship.

20. This Court has personal jurisdiction over the parties in this case. Defendants conduct business in this District and Geisinger is a citizen of this District by virtue of having its principal place of business located in this District.

21. Venue is proper in this District under 28 U.S.C. §1391(b) because Geisinger and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

A. Overview of Defendants

22. Geisinger claims to "serv[e] 1.2 million people in urban and rural communities across Pennsylvania." Geisinger "generates $10 billion in annual revenues across 134 care sites-including 10 hospital campuses and Geisinger Health Plan, with 600,000 members in commercial and government plans."[1]

23. Nuance provides healthcare technology services, including clinical solutions, diagnostic solutions, and revenue services. Nuance's "AI-powered solutions" are used "by 77% of hospitals and 10,000 healthcare organizations worldwide" and "capture 300 million patient stories

[1] *See* https://www.geisinger.org/about-geisinger/news-and-media/news-releases/2024/06/24/18/17/geisinger-provides-notice-of-nuances-data-security-incident (last visited July 15, 2024).

each year.[2]

24. While administering services, Geisinger receives and handles PHI/PII, which includes, *inter alia*, patients' full name, address, date of birth, Social Security number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

25. In order to receive services from Geisinger, Plaintiffs are required to entrust their highly sensitive PHI/PII to Defendant. Plaintiff entrusted this information to Geisinger with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

26. By obtaining, collecting, and storing Plaintiff's PHI/PII, Geisinger assumed legal and equitable duties and knew or should have known that Defendant was responsible for protecting Plaintiff's PHI/PII from unauthorized disclosure.

27. And, upon information and belief, Geisinger funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class members.

B. Geisinger Knew the Risks of Storing Valuable PHI/PII and the Foreseeable Harm to its Patients.

28. At all relevant times, Geisinger knew it was storing sensitive PHI/PII and that, as a result, its systems would be an attractive target for cybercriminals.

29. Geisinger provides its patients with a Noice of Privacy Practices (the "Geisinger Privacy Policy")[3] which "describes how medical information about [patients] may be used and

[2] *See* https://www.nuance.com/asset/en_us/collateral/healthcare/fact-sheet/fs-nuance-healthcare-fact-sheet-en-us.pdf (last visited July 15, 2024).
[3] *See* https://www.geisinger.org/about-geisinger/corporate/corporate-policies/website-privacy-policy (last visited July 15, 2024).

disclosed." Geisinger acknowledges it is "required to abide by the terms of this Notice." *Id.*

30. The Geisinger Privacy Policy states "Geisinger may only use and disclose your PHI pursuant to an authorization, or as otherwise permitted or required by law." *Id.* Geisinger says it will only use its patients' PHI for certain purposes, including treatment, healthcare operations, and billing and payment services.

31. Geisinger states, "We are required by law to maintain the privacy and security of your PHI. We will let you know promptly if a breach occurs that may have been compromised the privacy or security of your information."[4]

32. The Geisinger Privacy Policy claims Geisinger will only use or disclose patients' PHI/PII in ways other than specified in the Privacy Policy with a patient's "written permission or authorization."[5]

33. "Nuance collects personal data when we deliver our products, conduct marketing, and run our business operations." Nuance "use[s] the personal data that is processed within our Products, such as…data within medical data products…and any personal data contained within product usage data we collect, to deliver our Products sold to Nuance customers." "Nuance generally processes Product Personal Data on behalf of our healthcare, enterprise, and corporate customers."[6]

34. Nuance represents that if "follow[s] generally accepted standards to protect the personal data submitted to us, both during transmission and once it is received."

35. Defendants also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals

[4] *See* https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa/notice-of-privacy-practices-ghs (last visited July 15, 2024).
[5] *Id.*
[6] *See* https://www.nuance.com/about-us/company-policies/privacy-policies.html (last visited July 15, 2024).

whose PHI/PII was compromised, as well as intrusion into their highly private health information.

36. These risks are not theoretical. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[7]

37. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[8]

38. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022.

39. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[9]

40. Further, a 2022 report released by IBM Security stated that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[10]

41. Indeed, cyberattacks against the healthcare industry have been common for over the past ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PHI/PII." The FBI further warned

---

[7] *The healthcare industry is at risk*, SWIVELSECURE https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Apr. 17, 2023).

[8] *Id.*

[9] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, CYBERSECURITY NEWS (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

[10] *Cost of a Data Breach Report 2022*, IBM SECURITY, https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited Apr. 17, 2023).

that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[11]

42. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[12]

43. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[13]

44. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

45. PHI/PII is a valuable property right.[14] The value of PHI/PII as a commodity is

---

[11] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[12] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[13] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Apr. 17, 2023).

[14] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

measurable.[15] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[17] It is so valuable to identity thieves that once PHI/PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

46. As a result of their real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, PHI/PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

47. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future

[15] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle. /824192.

[16] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[17] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

harm."[18]

48. Even if stolen PHI/PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PHI/PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

49. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[19]

50. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PHI/PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

51. Based on the value of its patients' PHI/PII to cybercriminals and cybercriminals' propensity to target healthcare providers, Geisinger certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Defendants Breached its Duty to Protect its Patients' PHI/PII.

52. On June 24, 2024 Geisinger announced that it experienced a security incident

[18] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 17, 2023).

[19] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.guanotronic.com/~serge/papers/weis07.pdf.

disrupting access to its systems.

53. As noted above, the patient PHI/PII compromised in the Data Breach includes patient names, dates of birth, Social Security numbers, driver's license or state ID numbers, financial account and/or payment information, medical information, and health insurance information.

54. Like Plaintiff, other potential Class members received similar notices informing them that their PHI/PII was exposed in the Data Breach.

55. All in all, approximately 1,000,000 individuals with information stored on ER's system had their PHI/PII breached.

56. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic security procedures in order to protect its patients' PHI/PII.

D. FTC Guidelines Prohibit Defendants from Engaging in Unfair or Deceptive Acts or Practices.

57. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

58. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[20]

59. The FTC provided cybersecurity guidelines for businesses, advising that businesses

[20] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[21]

60. The FTC further recommends that companies not maintain PHI/PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[22]

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. Defendants failed to properly implement basic data security practices. Defendants failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PHI/PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

63. Geisinger was at all times fully aware of its obligations to protect patients' PHI/PII of because of its position as a healthcare provider, which gave it direct access to reams of patient PHI/PII. Geisinger is also aware of the significant repercussions that would result from its failure to do so.

E. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an

[21] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

[22] *Id.*

Increased Risk of Fraud and Identity Theft.

64. Cyberattacks and data breaches at healthcare companies like Geisinger are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

65. Researchers have found that among healthcare service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[23]

66. Researchers have further found that at healthcare service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[24]

67. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[25]

68. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a

[23] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour /science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[24] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 HEALTH SERVICES RESEARCH 971, 971-980 (2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[25] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

69. Theft of PHI/PII is serious. The FTC warns consumers that identity thieves use PHI/PII to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

70. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[26]

71. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the

[26] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Feb. 24, 2023).

victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

72. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

73. Moreover, theft of PHI/PII is also gravely serious because PHI/PII is an extremely valuable property right.[27]

74. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI/PII on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

75. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PHI/PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal

[27] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

losses to Plaintiff.

76. As discussed above, PHI/PII is such a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

77. Social Security Numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [28]

78. For instance, with a stolen Social Security Number, which is only one subset of the PHI/PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[29]

79. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[30] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[31] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number

---

[28] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added).

[29] *Id.*

[30] *Id.*

[31] *Id.* at 4.

was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

80. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[32]

81. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Geisinger is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

82. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[33] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[34]

83. These risks are both certainly impending and substantial. As the FTC has reported,

---

[32] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[33] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[34] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

if hackers get access to PHI/PII, they *will use it.*[35]

84. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. As with income tax returns, an individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

85. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[36]

86. Cybercriminals can post stolen PHI/PII on the cyber black-market for years following a data breach, thereby making such information publicly available.

87. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [37] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[38]

88. Identity theft victims must spend countless hours and large amounts of money

---

[35] *Id.*

[36] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

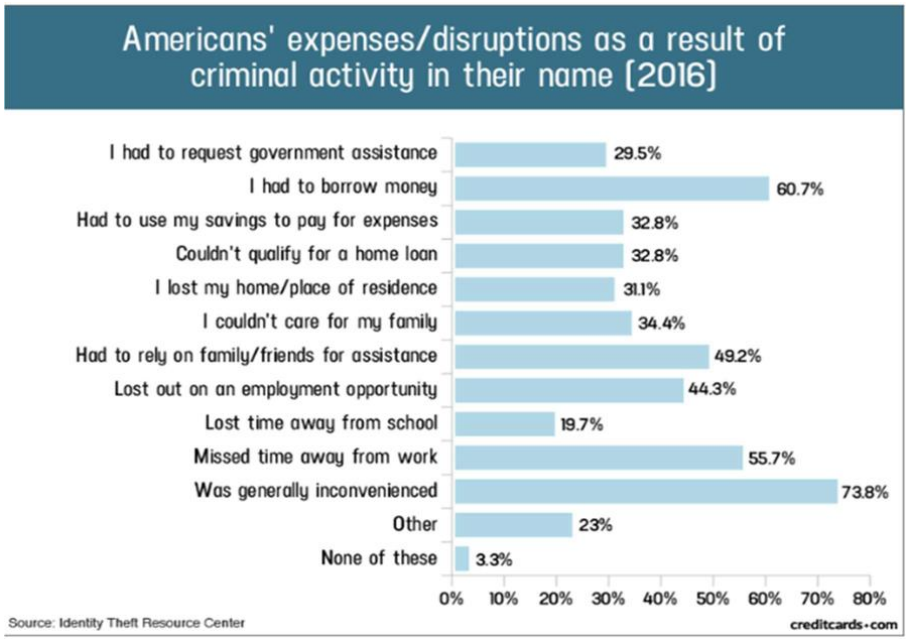
[37] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Apr. 17, 2023).

[38] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Apr. 17, 2023).

repairing the impact to their credit as well as protecting themselves in the future.[39]

89. It is within this context that Plaintiff must now live with the knowledge that their PHI/PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

90. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.



91. Victims of the Data Breach, like Plaintiff, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[40]

92. As a direct and proximate result of the Data Breach, Plaintiff has had her PHI/PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and

[39] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[40] *Id.*

continuing increased risk of harm from fraud and identity theft. Plaintiff must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on her everyday life, including purchasing identity theft and credit monitoring services every year for the rest of her life, placing "freezes" and "alerts" with credit reporting agencies, contacting her financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

93. Moreover, Plaintiff and Class members have an interest in ensuring that their PHI/PII, which remains in the possession of Defendants, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendants have shown themselves to be wholly incapable of protecting Plaintiff's PHI/PII.

94. Plaintiff and Class members also have an interest in ensuring that their personal information that was provided to Geisinger is removed from Geisinger's unencrypted files.

95. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, Geisinger knew or should have known about these dangers and strengthened its data security accordingly. Geisinger was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

F. Plaintiff Suffered Damages.

96. Geisinger received Plaintiff's and class members' PHI/PII in connection with providing certain medical services and treatment to them. In requesting and maintaining Plaintiff's PHI/PII for business purposes, Geisinger expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's and Class members' PHI/PII. Geisinger did not,

however, take proper care of Plaintiff's and Class members' PHI/PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Geisinger's inadequate security measures.

97. For the reasons mentioned above, Geisinger's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class members significant injuries and harm in several ways. Plaintiff and Class members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiff and Class members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

98. Once PHI/PII is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives because of Defendant's conduct.

99. Further, the value of Plaintiff's and Class members' PHI/PII has been diminished by its exposure in the Data Breach. Plaintiff and Class members did not receive the full benefit of their bargain when paying for medical services, and instead received services that were of a diminished value to those described in their agreements with Geisinger for the benefit and protection of Plaintiff and her respective PHI/PII. Plaintiff and Class members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually

received.

100. Plaintiff and Class members would not have obtained medical services from Geisinger, or paid the amount they did to receive such, had they known that Geisinger would negligently fail to adequately protect their PHI/PII. Indeed, Plaintiff and Class members paid for medical services with the expectation that Geisinger would keep their PHI/PII secure and inaccessible from unauthorized parties. Plaintiff and Class Members would not have obtained services from Geisinger had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PHI/PII from criminal theft and misuse.

101. As a result of Defendants' failures, Plaintiff and Class Members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PHI/PII.

102. Further, because Defendant delayed in notifying Plaintiff about the Data Breach for nearly four months, Plaintiff was unable to take affirmative steps during that time period to attempt to mitigate any harm or take prophylactic steps to protect against injury.

103. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[41]

104. "Actors buying and selling PHI/PII from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's

[41] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Apr. 17, 2023).

utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[42]

105. Plaintiff is also at a continued risk because their information remains in Geisinger's computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Geisinger fails to undertake the necessary and appropriate security and training measures to protect its patients' PHI/PII.

106. In addition, Plaintiff and Class members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ALLEGATIONS

107. Plaintiff brings all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All individuals within the United States whose PHI/PII was accessed in the Data Breach (the "Class").

108. Excluded from the Class are Defendants, its subsidiaries and affiliates, officers and directors, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

109. This proposed Class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the Class definition in an amended pleading or when she moves for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

[42] David, *supra* note 67.

110. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiff is informed and believes, and thereon alleges, that there are at minimum, hundreds of thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendants' records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 1,000,000 individuals.

111. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Defendants failed to timely notify Plaintiff of the Data Breach;

b. Whether Defendants had a duty to protect Plaintiff's and Class Members' PHI/PII;

c. Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PHI/PII, and breached its duties thereby;

d. Whether Defendants breached their fiduciary duty to Plaintiff and the Class;

e. Whether Defendants breached their duty of confidence to Plaintiff and the Class;

f. Whether Defendants violated their own Privacy Practices;

g. Whether Defendants entered into a contract implied in fact with Plaintiff and the Class;

h. Whether Defendants breached that contract by failing to adequately safeguard Plaintiff's and Class members' PHI/PII;

i. Whether Defendants were unjustly enriched;

j. Whether Plaintiff and Class members are entitled to damages as a result of

Defendants' wrongful conduct; and

k. Whether Plaintiff and Class members are entitled to restitution as a result of Defendants' wrongful conduct.

112. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class all had information stored in Geisinger's System, each having their PHI/PII exposed and/or accessed by an unauthorized third party.

113. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex Class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel have adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

114. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendants have acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

115. **Superiority, Fed. R. Civ. P. 23(b)(3):** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of

separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

116. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

117. Likewise, issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendants failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PHI/PII;

c. Whether Defendants' security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PHI/PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data

Breach.

118. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

FIRST CAUSE OF ACTION
NEGLIGENCE
(Plaintiff on behalf of the Class)

119. Plaintiff restates and reallege the preceding allegations above as if fully alleged herein.

120. Plaintiff brings this claim individually and on behalf of the Class.

121. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in safeguarding and protecting their PHI/PII in its possession, custody, and control.

122. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

123. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendants. By collecting and storing valuable PHI/PII that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

124. Defendants' duty also arose from Defendants' position as a healthcare vendor. Defendants hold themselves out as trusted providers of services for the healthcare industry, and thereby assume a duty to reasonably protect patients' information.

125. Defendants breached the duties owed to Plaintiff and Class Members and thus were negligent. As a result of a successful attack directed towards Defendants that compromised

Plaintiff's and Class members' PHI/PII, Defendants breached their duties through some combination of the following errors and omissions that allowed the data compromise to occur:

(a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PHI/PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PHI/PII.

126. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PHI/PII would not have been compromised.

127. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries, including, but not limited to:

a. Theft of their PHI/PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PHI/PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PHI/PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PHI/PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PHI/PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PHI/PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

128. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(Plaintiff on behalf of the Class)

129. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

130. Plaintiff brings this claim individually and on behalf of the Class.

131. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants for failing to use reasonable measures to protect PHI/PII. Various FTC publications and orders also form the basis of Defendants' duty.

132. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PHI/PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PHI/PII it obtained and stored and the foreseeable consequences of a data breach involving PHI/PII of its patients.

133. Plaintiff and members of the Class are consumers within the Class of persons Section 5 of the FTC Act was intended to protect.

134. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

135. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act and Part 2 was intended to guard against.

136. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including

compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(Plaintiff on behalf of the Class)

137. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

138. Plaintiff and Class Members have an interest, both equitable and legal, in the PHI/PII about them that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

139. As a provider of electronic health record software, and recipient of patients' PHI/PII, Defendants have a fiduciary relationship to its customers, including Plaintiff and the Class members.

140. Because of that fiduciary relationship, Defendants were provided with and stored private and valuable PHI/PII related to Plaintiff and the Class. Plaintiff and the Class were entitled to expect their information would remain confidential while in Defendants' possession.

141. Defendants owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PHI/PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

142. As a result of the parties' fiduciary relationship, Defendants had an obligation to maintain the confidentiality of the information within Plaintiff's and the Class Members' medical records.

143. Defendants' customers, including Plaintiff and Class members, have a privacy interest in personal medical matters, and Geisinger had a fiduciary duty not to disclose medical

data concerning its patients.

144. As a result of the parties' relationship, Defendants had possession and knowledge of confidential PHI/PII of Plaintiff and Class Members, information not generally known.

145. Plaintiff and Class members did not consent to nor authorize Defendants to release or disclose their PHI/PII to unknown criminal actors.

146. Defendants breached its fiduciary duties owed to Plaintiff and Class Members by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PHI/PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its patients; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PHI/PII.

147. But for Defendants' wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their PHI/PII would not have been compromised.

148. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered injuries, including:

a. Theft of their PHI/PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PHI/PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PHI/PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PHI/PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PHI/PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PHI/PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

149. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(Plaintiff on behalf of the Class)

150. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

151. Plaintiff and Class Members have an interest, both equitable and legal, in the PHI/PII about them that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

152. As a healthcare provider, Defendants had a special relationship to its customers,

like Plaintiff and the Class Members.

153. Plaintiff and Class Members provided Defendants with their personal and confidential PHI/PII under both the express and/or implied agreement of Defendants to limit the use and disclosure of such PHI/PII.

154. Defendants owed a duty to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PHI/PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

155. As a result of the parties' relationship, Defendants had possession and knowledge of confidential PHI/PII and confidential medical records of Plaintiff and Class Members.

156. Plaintiff's and Class Members' PHI/PII is not generally known to the public and is confidential by nature.

157. Plaintiff and Class Members did not consent to nor authorize Defendants to release or disclose their PHI/PII to an unknown criminal actor.

158. Defendants breached the duties of confidence it owed to Plaintiff and Class members when their PHI/PII were disclosed to unknown criminal hackers.

159. Defendants breached its duties of confidence by failing to safeguard Plaintiff's and Class members' PHI/PII, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PHI/PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key

controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; (h) storing PHI/PII and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' PHI/PII and medical records/information to a criminal third party.

160. But for Defendants' wrongful breach of its duty of confidences owed to Plaintiff and Class Members, their privacy, confidences, and PHI/PII would not have been compromised.

161. As a direct and proximate result of Defendants' breach of Plaintiffs' and Class Members' confidences, Plaintiff and Class members have suffered injuries, including:

a. The erosion of the essential and confidential relationship between Defendants – as health care services providers – and Plaintiff and Class Members as patients;

b. Theft of their PHI/PII;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PHI/PII;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual

and future consequences of the Geisinger Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PHI/PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PHI/PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PHI/PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

j. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendants.

162. Additionally, Defendants received payments from Plaintiff and Class Members for services with the understanding that Defendants would uphold its responsibilities to maintain the confidences of Plaintiff's and Class Members' private medical information.

163. Defendants breached the confidence of Plaintiff and Class Members when it made

an unauthorized release and disclosure of their confidential medical information and, accordingly, it would be inequitable for Defendants to retain the benefit at Plaintiff's and Class Members' expense.

164. As a direct and proximate result of Defendants' breach of its duty of confidences, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(Plaintiff on behalf of the Class)

165. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

166. Plaintiff and Class members had a reasonable expectation of privacy in the PHI/PII Defendants mishandled.

167. Defendants' conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion under common law.

168. By intentionally failing to keep Plaintiff's and Class Members' PHI/PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiff's and Class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class Members' private affairs in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class Members.

169. Defendants knew that an ordinary person in Plaintiff's or Class Members' position would consider Defendants' intentional actions highly offensive and objectionable.

170. Defendants invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by intentionally misusing and/or disclosing their PHI/PII without their informed, voluntary, affirmative, and clear consent.

171. Defendants intentionally concealed from and delayed reporting to Plaintiff and Class members a security incident that misused and/or disclosed their PHI/PII without their informed, voluntary, affirmative, and clear consent.

172. The conduct described above was at or directed at Plaintiff and the Class Members.

173. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their PHI/PII was unduly frustrated and thwarted. Defendants' conduct amounted to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

174. In failing to protect Plaintiff's and Class members' PHI/PII, and in intentionally misusing and/or disclosing their PHI/PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

175. As a direct and proximate result of Defendnats' conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in

an amount to be proven at trial.

SIXTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Plaintiff on behalf of the Class)

176. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

177. Plaintiff brings this claim individually and on behalf of the Class.

178. When Plaintiff and members of the Class provided their PHI/PII to Geisinger in exchange for healthcare services, they entered into implied contracts with Defendants, under which Defendants agreed to take reasonable steps to protect Plaintiff's and Class Members' PHI/PII, comply with it statutory and common law duties to protect Plaintiff's and Class Members' PHI/PII, and to timely notify them in the event of a data breach.

179. Geisinger solicited and invited Plaintiff and Class Members to provide their PHI/PII as part of Geisinger's provision of healthcare services. Plaintiff and Class Members accepted Geisinger's offers and provided their PHI/PII to Geisinger.

180. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with its statutory and common law duties to adequately protect Plaintiff's and Class Members' PHI/PII and to timely notify them in the event of a data breach.

181. Defendants implied promise to safeguard patient PHI/PII is evidenced by, *e.g.*, the representations in Defendants' Notice of Privacy Practices set forth above.

182. Plaintiffs and Class Members paid money to Geisinger in order to receive healthcare services. Plaintiff and Class Members reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do

so.

183. Plaintiff and Class members would not have provided their PHI/PII to Geisinger had they known that Defendants would not safeguard their PHI/PII, as promised, or provide timely notice of a data breach.

184. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendants.

185. Defendants breached their implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' PHI/PII and by failing to provide them with timely and accurate notice of the Data Breach.

186. The losses and damages Plaintiff and Class members sustained, include, but are not limited to:

a. Theft of their PHI/PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PHI/PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and

imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PHI/PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PHI/PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PHI/PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PHI/PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

187. As a direct and proximate result of Defendants' breach of contract, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SEVENTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiff on behalf of the Class)

188. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

189. Plaintiff brings this claim individually and on behalf of the Class in the alternative to Plaintiff's Implied Contract claim.

190. Upon information and belief, Defendants funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

191. As such, a portion of the payments made by or on behalf of Plaintiff's and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

192. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased healthcare services from Geisinger and/or its agents and in so doing provided Defendants with their PHI/PII. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their PHI/PII protected with adequate data security.

193. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the PHI/PII of Plaintiff's and Class members for business purposes.

194. In particular, Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class members' PHI/PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize its own profits over the requisite security.

195. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

196. Defendants failed to secure Plaintiff's and Class Members' PHI/PII and, therefore, did not provide full compensation for the benefit Plaintiff's and Class Members provided.

197. Defendants acquired the PHI/PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

198. If Plaintiff and Class Members knew that Defendants had not reasonably secured their PHI/PII, they would not have agreed to provide their PHI/PII to Defendants.

199. Plaintiff and Class Members have no adequate remedy at law.

200. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered injuries, including, but not limited to:

a. Theft of their PHI/PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PHI/PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent

charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PHI/PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PHI/PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PHI/PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PHI/PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

201. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

202. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and

Class Members overpaid for Defendants' services.

EIGHTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiff on behalf of the Class)

203. Plaintiff restates and realleges the preceding allegations the paragraphs above as if fully alleged herein.

204. Plaintiff brings this claim individually and on behalf of the Class.

205. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

206. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' PHI/PII, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their PHI/PII. Plaintiff and the Class remain at imminent risk that additional compromises of their PHI/PII will occur in the future.

207. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect consumers' PHI/PII.

208. Defendants still possesses Plaintiff's Class members' PHI/PII.

209. Defendants have made no announcement that it has changed its data storage or security practices relating to the storage of Plaintiff's and Class Members' PHI/PII.

210. To Plaintiff's knowledge, Defendants have made no announcement or notification

that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

211. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Geisinger. The risk of another such breach is real, immediate, and substantial.

212. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs at Geisinger, Plaintiff and Class Members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

213. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Geisinger, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other consumers whose PHI/PII would be further compromised.

214. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that ER implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Geisinger's systems on a periodic basis, and ordering Geisinger to promptly correct any problems or issues detected by such third-party security

auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying PHI/PII not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, pray for relief as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiff as a Class Representative and her counsel as Class Counsel;

b. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI/PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully

retained as a result of Defendants' wrongful conduct;

e. Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and,

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded by Plaintiff on all claims so triable.

Dated: July 15, 2024 Respectfully submitted,

/s/ Marc H. Edelson

Marc H. Edelson (PA 51834)
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940
T: (215) 867-2399
medelson@edelson-law.com

Attorneys for Plaintiff and the Putative Class